DIGITAL SIGNATURE SYSTEM AND METHOD

Inventor:
Mir Hajmiragha
Jeffrey Cochran

PRIORITY CLAIM

This application claims priority from Provisional Patent No. 60/213,204, filed June 21, 2000.

FIELD OF THE INVENTION

This invention relates to digital signatures, and more particularly to digital signatures in documents.

BACKGROUND OF THE INVENTION

A digital signature is an electronic rather than a written signature that can be used by someone to authenticate the identity of the sender of a message or of the signer of a document. It can also be used to ensure that the original content of the message or document that has been conveyed is unchanged. Additional benefits to the use of a digital signature are that it is easily transportable, cannot be easily repudiated, cannot be imitated by someone else, and can be automatically time-stamped.

A digital signature can be used with any kind of message, whether it is encryption or not, simply so that the receiver can be sure of the sender's identity and that the message arrived intact. A digital certificate contains the digital signature of the certificate-issuing authority so that anyone can verify that the certificate is real.

Assume you were going to send the draft of a contract to your lawyer in another town. You want to give your lawyer the assurance that it was unchanged from what you sent and that it is really from you. First, you copy-and-paste the contract into an e-mail note. Using hashing software, you obtain a message hashing (mathematical summary) of the contract. A private key that you have previously obtained from a public-private key (certificate-issuing) authority encrypts the hash. The encrypted hash becomes the digital signature of the message. When the lawyer receives the document with the message, the lawyer's system makes a hash of the received document. The lawyer then uses your public key to decrypt the digital signature of the message (i.e. the encrypted hash) to obtain a hash. If the created hash and the decrypted hash match, the received message is valid.

This method is an effective tool for securely transmitting digitally signed documents. However, many times with contracts there exists a requirement to have viewers of the document initial various important parts of the document. Therefore, there exists a need for imparting initialing information in a digitally signed document in order to make the digital signing process more like what is performed in paper versions.

SUMMARY OF THE INVENTION

The present invention is a digital signature system and method that provides digital document signing and signing of selected text within the document. The system includes a plurality of remotely located computer-based systems coupled to a document computer-based system over a public data network. The remotely located computer-based systems include a user interface component for displaying an electronic document that the user of the computer-based system desires to assign signing functions thereto, and for designating one or more blocks of text for signature tasks, a processing component for uniquely identifying the designated blocks of text, and a browser component. The browser component includes an assigning component for assigning one or more other users to one or more of the blocks text in a registered document, and a signing component for allowing review of the assigning blocks of text, that are assigned to the user, for selecting at least one of an acceptance option

or a decline option for each of the assigned blocks of text, and for executing a digital signature of the blocks of text. The document system includes a registering component for identifying designated blocks of text, and for verifying the correctness of uniquely identified blocks of text, a storing component for storing the users assigned to the blocks of text of a registered document, a retrieval component for allowing retrieval of documents with previously assigned signature tasks and for allowing retrieval of the stored digital signatures of a document and the stored users' selections, a signing component for allowing review of the assigning blocks of text, that are assigned to the user, for selecting at least one of an acceptance option or a decline option for each of the assigned blocks of text, and for executing a digital signature of the blocks of text, and a history component for storing transaction history of registered documents. The history component includes a first storing component for storing digital signatures of documents, and a second storing component for storing the users' selections of the acceptance or decline option.

As will be readily appreciated from the foregoing summary, the invention provides a method and system for allowing users at remote locations to sign and designate for signature blocks of text of a document in a secure environment.

BRIEF DESCRIPTION OF THE DRAWINGS

The preferred embodiment of this invention is discussed in detail below with reference to the following drawings.

FIGURE 1 is a system block diagram formed in accordance with the present invention;

FIGURE 2 is a flow diagram for designation a document and portions thereof for signing;

FIGURE 3 is a flow diagram for signing a document;

FIGURE 4 is a flow diagram for illustrating tag data structure creation;

FIGURE 5 is a partial screen shot of document application program for implementing the present invention;

FIGURES 6-8 are screen shots of window used in conjunction with the document application program shown in FIGURE 5;

FIGURE 9 is a web page viewed at a user's system for uploading documents to a server over a network; and

FIGURE 10 is a web page viewed at a user's system for signing a document stored at the server over the network.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

The present invention is a digital signature system and method for digitally signing documents. An example system 20 is shown in FIGURE 1. The system 20 includes a digital signature server 22, such as that provided by DocuTouch™, coupled to a signature repository 24 and a document repository 26. The digital signature server 22 is also coupled to a plurality of user systems 28 over a public or private data network 30. In an alternate embodiment, one or more document repositories 34 are connected to the digital signature server 22 over the network 30. The signature repository 24 stores various information pertaining to subscribing users' signature information, such as digital certificate information. The document repository 26 stores registered document information. A method is implemented for associating a digital signature with a document stored in the repository 26. The local document repository 26 includes a referenced path to another storage location; document repositories 34.

As shown in FIGURE 2, a user using a user system 28 creates or retrieves an electronic document that they wish to designate for review and signing by others, see block 80. An example of electronic documents are parseable documents, such as those created in word processing programs (e.g. MS Word, Adobe Reader, etc.). Next, at block 82, the user identifies one or more blocks of text requiring review by others. An example of identifying a block of text is described in FIGURE 4 below. At block 83, one or more tag data structures are created for each identified block of text and associated with the document the text is from. Tag data structure creation is described by example in FIGURE 4. At block 84, the document with the identified one or more blocks of text is sent by the user to the digital signature server 22 via the network 30 for uploading and processing, thereby registering the document, see FIGURE 9. At block 86, the digital signature server 22 finds the identified blocks of text within the document according to the created tag data structures that are associated with the document. The digital signature server 22 or a processing component thereof analyzes a registered document for associated created tag data structures and/or message digests. Then, at block 88, the user interacting with a user interface, described below in FIGURE 10, assigns tasks for others to perform on the document or on a the found blocks of text within the document. Once the user has completed the assignment of tasks, the digital signature server 22 makes the document available to those users that have been assigned tasks.

FIGURE 3 illustrates a method a user performs in order to complete tasks assigned to them for documents registered with the digital signature server 22. First, at block 100 the user connects to the digital signature server 22. In one aspect embodiment of the present invention the connection is a connection over the Internet and requires that the user using a user system 28 logs onto a web site hosted by the digital signature server 22. In one embodiment, the user has preregistered with the server 22 and has received a password required for later logons. Next, at block 102, the user receives notification of documents with assigned tasks not yet before. In one embodiment, a user interface or web page identifies a list of documents requiring tasks to be performed by that user. Various other information is associated with assigned tasks, such as deadline dates, others required to review and sign documents history information. Then, at block 103, the user selects a document with assigned task or tasks not yet performed. At decision block 104, if a task requiring the user to perform is not a signing task, the digital signature server 22 will request that the user perform the desired task. However, if an assigned task is a signing task, then, at block 106, the user reviews any identified blocks of text requiring action. At block 108, the user selects an option associated with each of the identified blocks of text within the document. At decision block 110, if there remains options associated with identified blocks text with in the document that have not been completed the process returns to block 106 until the user completes the selection of the options associated with all the identified blocks text. Once the user has completed the selection of all options associated with all the identified blocks text, then, at block 112, the electronic signing of the document is performed. FIGURE 10 shows example web page a user might see when reviewing for the purpose of applying a digital signature.

As shown in FIGURE 4, creation of a tag data structure (block 83 from FIGURE 2) includes, at block 150, the user system 28 to generate a unique identifier for a block of text. Next, at block 152, the user enters a reference name for each block of text. In an alternate embodiment a default of the first n number of words of the block of text is automatically entered. Then, at block 154, a message digest is created by a hashing algorithm that is stored within the user system 28. At block 156, the message digest, reference name, and the unique identifier (the tag data structure) are stored within the user system 28, thereby completing the last component of the tag data structure creation. A unique identifier is generated by an identifier application, such as that generated by Microsoft's Global Unique Identifier program. In one embodiment the

unique identifier is a 16 byte structure. The tag data structure includes a version mask, the message digest, the hashing algorithm used to generate the message digest, the reference name, the text of the block.

FIGURE 5 illustrates a partial screenshot of an application program window 180, that allows a user to identify blocks of text within a document. As shown in the example of FIGURE 5, the present invention is embedded into Microsoft Word, but could be embedded or associated with any other type of word processing application program, or could be a stand-alone application program. In this example, the user has selected a document 186 (the Declaration of Independence) for assigning signature tasks to. This document 186 is displayed in a workspace area of the window 180. The application program window 180 includes various user interface components, such as user interface buttons 190 implemented within a button bar of the window 180 and within commands in a pull-down menu 191 implemented within a pull-down menu section. In this example, the user has are already designated a block of text within the brackets 192 and 194 requiring signature. An icon 196 is displayed adjacent the identified block of text of the document, thereby providing a user interface indication of an identified block of text. When a user identifies a block of text, semaphores are created for identifying the beginning and ending of the block of text. The semaphores are uniquely identified and serialized in the document. The ending semaphore is used as the print tag for imbedding digital signatures in the document without invalidating associated message digest. After the document has been registered and signed by another, the associated ending semaphore is linked to a website that displays the signature block. The document is parsed during registration with the server 22, and each block is digested and stored in the database as a signature candidate. The user then assigns a signature activity to each block of text. The signatures are viewable by all parties as a live link with the server 22, as well as printable during the publication process. Live-links are addresses that allow users to jump to a given web page, document, or other real-time information.

FIGURE 6 illustrates a tag name insert window 204 presented after activation of an associated command or button in window 180. The tag name insert window 204 includes an interactive tag name entry space 206 that presents a default tag name for a block of text or a user defined tag name. A tag refers to a block of text.

FIGURE 7 illustrates a GOTO window 210 presented after activation of an associated command or button. The GOTO window 210 includes a sub-window 212 that presents a list of

the identified blocks of text within the document. After the user highlights one of the identified blocks of text within the sub-window 212 and activates a GoTo button 214 the selected name for the block text, the actual block text is displayed in the window 180.

As shown in FIGURE 8, a delete tag window 220 allows a user to highlight a tag name within a sub-window 222 and delete the signing tag (data structure) associated with the block text by selecting a delete button 224.

FIGURE 9 is a screen shot of an example web pages 240 for sending a document to the server 22 for registration. The web page 240 includes a menu area 242 and a document upload area 244. The menu area 242 includes hyperlinks to other server supported web pages that provide other document processing services. The document upload area 244 includes a select documents area 246 that includes a plurality of document name entry/browse button pair 248. The document upload area 244 also includes a document attribute assigning area 256 that allows a user to assign various categorical attributes to selected documents. A document owner area 260 included in the document upload area 244 includes an entry window 262 for entering names of owners for the selected documents. An option area 268 also included in the document upload area 244 allows the user to assign various document processing options to the selected documents.

FIGURE 10 illustrates a document review and signing web page 290. The web page 290 includes a main menu area 292 and a document review and sign area 294. The main menu area 292 hyperlinks to other server supported web pages that provide other document processing services. The document review and sign area 294 presents blocks of text in a display area 296. The block of text displayed in the display area 296 of this example is the same block of text from the Declaration of Independence.doc that was selected in FIGURE 5. Option buttons 298 (I Agree 300 and I Decline 302) are displayed adjacent to the display area 296. If the user agrees to the displayed block of text, the user selects the I Agree 300. If the user does not agree to the displayed block of text, the user selects the I Decline 302. The document review and sign area 294 also includes a submit button 306 and various navigational buttons 308. Selection of the submit button 306 initiates the digital signing of the document with the results of the option buttons' selections for all the blocks of text. Other user interface buttons, display layouts may be implemented without departing from the spirit and scope of the invention.

Standards for digital signature are defined within the Public-Key Cryptography Standards (PKCS). Public-key cryptography is an asymmetric cryptography technology. In asymmetric encryption and decryption, two keys are used. Data encrypted with the either key may be decrypted by using the other. Typically, the value of one key is kept secure (generally referred to as the private key), while the second keys value is widely shared (the public key). Digital signature technology exploits this implementation.

When a user activates a signing of a document, a browser application program on the user's system 28 reads the user's private key from secure storage on the user's system 28. The private key is wrapped within a previously issued certificate and maintained within the user's system 28. The data to be signed is encrypted by using the private key.

While the preferred embodiment of the invention has been illustrated and described, it will be appreciated that various changes can be made without departing from the spirit and scope of the invention.